

UNITED STATES DISTRICT COURT
 for the
 Southern District of Ohio

FILED
 RICHARD W. HAGEL
 CLERK OF COURT

2020 JAN 30 AM 10:57

U.S. DISTRICT COURT
 SOUTHERN DIST. OHIO
 WESTERN DIV. DAYTON

3:20 mj 055

In the Matter of the Search of

(Briefly describe the property to be searched
 or identify the person by name and address)

HP Stream Laptop, Model 11-ah011wm, serial number
 5CD84382N2, currently located at the FBI, 7747 Clyo
 Road, Centerville, OH, 45459

Case No.

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Southern District of Ohio, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- evidence of a crime;
- contraband, fruits of crime, or other items illegally possessed;
- property designed for use, intended for use, or used in committing a crime;
- a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

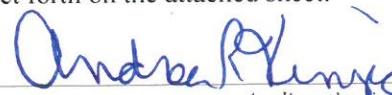
Code Section

Offense Description

See Attachment C

The application is based on these facts:
 See Attached Affidavit

- Continued on the attached sheet.
- Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


 Andrea R. Kinzig
 Applicant's signature

Andrea R. Kinzig, Special Agent

Printed name and title


 Sharon L. Ovington
 Judge's signature

Sharon L. Ovington, U.S. Magistrate Judge

Printed name and title

Sworn to before me and signed in my presence.

Date: 1-30-20

City and state: Dayton, Ohio

ATTACHMENT A

DESCRIPTION OF PROPERTY TO BE SEARCHED

The property to be searched is a HP Stream Laptop, Model 11-ah011wm, serial number 5CD84382N2 (“SUBJECT DEVICE”). The SUBJECT DEVICE is currently located at the Federal Bureau of Investigation, 7747 Clyo Road, Centerville, Ohio, 45459.

This warrant authorizes the forensic examination of the SUBJECT DEVICE for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED AND SEARCHED

Items evidencing violations of 18 U.S.C. §§ 2252(a)(4)(B) and (b)(1) and 2252A(a)(5)(B) and (b)(1) (possession and attempted possession of child pornography) and 18 U.S.C. §§ 2252(a)(2)(B) and (b)(1) and 2252A(a)(2) and (b)(1) (receipt and attempted receipt of child pornography), including but not limited to the following:

1. Any visual depictions and records related to the possession and receipt of child pornography.
2. Any visual depictions of minors.
3. Any Internet history indicative of searching for child pornography.
4. Any Internet or cellular telephone communications (including email, social media, online chat programs, etc.) with others in which child exploitation materials and offenses are discussed and/or traded.
5. Any Internet or cellular telephone communications (including email, social media, etc.) with minors.
6. Evidence of utilization of email accounts, social media accounts, online chat programs, and peer-to-peer file sharing programs.
7. Lists of computer and Internet accounts, including user names and passwords.
8. Any information related to the use of aliases.
9. Evidence of user attribution showing who used or owned the SUBJECT DEVICE at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

The authorization includes the seizure and search of electronic data to include deleted data, remnant data and slack space.

ATTACHMENT C

<u>Code Section</u>	<u>Offense Description</u>
18 U.S.C. §2252(a)(4)(B) & (b)(1)	Possession of Child Pornography
18 U.S.C. §2252A(a)(5)(B) & (b)(1)	Possession of Child Pornography
18 U.S.C. §2252(a)(2)(B) & (b)(1)	Receipt of Child Pornography
18 U.S.C. §2252A(a)(2) & (b)(1)	Receipt of Child Pornography

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Andrea R. Kinzig, being duly sworn, depose and state the following:

INTRODUCTION

1. I make this Affidavit in support of an Application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property — an electronic device — which is currently in law enforcement's possession, and the extraction from that property of electronically stored information described in Attachment B.
2. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), and have been so employed since 2005. I am currently assigned to the Dayton, Ohio Resident Agency of the Cincinnati Field Office. In connection with my official duties, I investigate violations of federal criminal laws, including offenses pertaining to the illegal production, distribution, receipt, and possession of child pornography (in violation of 18 U.S.C. §§ 2252(a) and 2252A). I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in various forms of media, including computer media.
3. Along with other agents, officers, and investigators of the Sidney (Ohio) Police Department and FBI, I am currently involved in an investigation of child pornography offenses committed by CHARLES LEE FRAZIER (hereinafter referred to as "FRAZIER"). This Affidavit is submitted in support of an Application for a search warrant for the following:
 - a. HP Stream Laptop, Model 11-ah011wm, serial number 5CD84382N2 (hereinafter referred to as the "**SUBJECT DEVICE**").
4. The **SUBJECT DEVICE** is currently located at the Federal Bureau of Investigation, 7747 Clyo Road, Centerville, Ohio, 45459. The purpose of the Application is to seize evidence of the following violations:
 - a. 18 U.S.C. §§ 2252(a)(4)(B) and (b)(1) and 2252A(a)(5)(B) and (b)(1), which make it a crime to possess or attempt to possess child pornography; and
 - b. 18 U.S.C. §§ 2252(a)(2)(B) and (b)(1) and 2252A(a)(2) and (b)(1), which make it a crime to receive or attempt to receive child pornography through interstate commerce.

5. The items to be searched for and seized are described more particularly in Attachment B hereto and are incorporated by reference.
6. As part of the investigation, I have reviewed documentation and reports provided by and discussed information with other agents, officers, and investigators involved in the investigation. For purposes of this Affidavit, I have not distinguished between information of which I have direct knowledge and that of which I have hearsay knowledge.
7. This Affidavit does not contain every fact known to the investigation, but only those deemed necessary to demonstrate sufficient probable cause to support the search of the **SUBJECT DEVICE**.
8. As a result of the instant investigation described more fully below, there is probable cause to believe that evidence of a crime; contraband, fruits of crime, or other items illegally possessed; property designed for use, intended for use, or used in committing a crime or violations of federal law; including violations of 18 U.S.C. §§ 2252(a)(4)(B) and (b)(1), 2252A(a)(5)(B) and (b)(1), 2252(a)(2)(B) and (b)(1), and 2252A(a)(2) and (b)(1), are present within the information located on the **SUBJECT DEVICE**.

PERTINENT FEDERAL CRIMINAL STATUTES

9. 18 U.S.C. § 2252(a)(4)(B) and (b)(1) states that it is a violation for any person to knowingly possess, or knowingly access with the intent to view, one or more matters which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct, or attempt to do so.
10. 18 U.S.C. § 2252A(a)(5)(B) and (b)(1) states that it is a violation for any person to knowingly possess, or knowingly access with intent to view, any book, magazine, periodical, film, videotape, computer, disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer, or attempt to do so.
11. 18 U.S.C. § 2252(a)(2)(B) and (b)(1) states that it is a violation for any person to knowingly receive or distribute any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, shipped, or transported in or

affecting interstate or foreign commerce or which contains materials which have been mailed or so shipped or transported by any means, including by computer, or to knowingly reproduce any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct, or attempt to do so.

12. 18 U.S.C. § 2252A(a)(2) and (b)(1) states that it is a violation for any person to receive or distribute – (A) any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; and (B) any material that contains child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer, or attempt to do so.

BACKGROUND INFORMATION

Definitions

13. The following definitions apply to this Affidavit and Attachment B to this Affidavit:

- a. **“Child Pornography”** includes the definition in Title 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).
- b. **“Visual depictions”** include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image (see 18 U.S.C. § 2256(5)).
- c. **“Minor”** means any person under the age of eighteen years (see 18 U.S.C. § 2256(1)).
- d. **“Sexually explicit conduct”** means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person (see 18 U.S.C. § 2256(2)).

- e. “**Internet Service Providers**” or “**ISPs**” are commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth that the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and password.
- f. An “**Internet Protocol address**”, also referred to as an “**IP address**”, is a unique numeric address that computers or electronic devices use in order to communicate with each other on a computer network utilizing the Internet Protocol (IP) standard. Every computer or device connected to the Internet is referenced by a unique IP address. An IP address can be thought of as the equivalent to a street address or a phone number, just as each street address and phone number uniquely identifies a building or telephone. IP addresses are composed of four sets of digits known as “octets,” ranging in value from 0-255, separated by decimal points. An example of an IP address is 192.168.10.102. There are two types of IP addresses; static and dynamic. A static address is permanently assigned to a particular device and as a practical matter never changes. A dynamic address provided by an Internet service provider to a client computer is valid only for the duration of the session that the client computer is connected to the Internet (or other network).
- g. A network “**server**,” also referred to as a “**host**,” is a computer system that has been designated to run a specific server application or applications and provide requested services to a “client” computer. A server can be configured to provide a wide variety of services over a network, including functioning as a web server, mail server, database server, backup server, print server, FTP (File Transfer Protocol) server, DNS (Domain Name System) server, to name just a few.
- h. A “**client**” is the counterpart of a server or host. A client is a computer system that accesses a remote service on another computer by some kind of network. Web browsers (like Internet Explorer or Safari) are clients that connect to web servers and retrieve web pages for display. E-mail clients (like Microsoft Outlook

or Eudora) retrieve their e-mail from their Internet service provider's mail storage servers.

- i. **“Domain Name”** refers to the common, easy to remember names associated with an Internet Protocol address. For example, a domain name of “www.usdoj.gov” refers to the Internet Protocol address of 149.101.1.32. Domain names are typically strings of alphanumeric characters, with each level delimited by a period. Each level, read backwards – from right to left – further identifies parts of an organization. Examples of first level, or top level domains are typically “.com” for commercial organizations, “.gov” for the governmental organizations, “.org” for organizations, and, “.edu” for educational organizations. Second level names will further identify the organization, for example “usdoj.gov” further identifies the United States governmental agency to be the Department of Justice. Additional levels may exist as needed until each machine is uniquely identifiable. For example, www.usdoj.gov identifies the World Wide Web server located at the United States Department of Justice, which is part of the United States government. The Domain Name System, also referred to DNS, is a system of servers connected to each other using a common system of databases that resolve a particular domain name, such as “www.usdoj.gov,” to its currently assigned IP address (*i.e.*, 149.101.1.32), to enable the follow of traffic across the Internet.
- j. **“Log Files”** are records automatically produced by computer programs to document electronic events that occur on computers. Computer programs can record a wide range of events including remote access, file transfers, logon/logoff times, and system errors. Logs are often named based on the types of information they contain. For example, web logs contain specific information about when a website was accessed by remote computers; access logs list specific information about when a computer was accessed from a remote location; and file transfer logs list detailed information concerning files that are remotely transferred.
- k. **“Hyperlink”** (often referred to simply as a “link”) refers to a navigation element in a web page or document that automatically brings the referred information (a.k.a. “resource”) to the user when the navigation element is selected by the user. Hyperlinks are part of the foundation of the World Wide Web, but are not limited to a website for HTML.
- l. **“Website”** consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

- m. "**Uniform Resource Locator**" or "**Universal Resource Locator**" or "**URL**" is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website's home page file in the Web browser's address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.
- n. The terms "**records**," "**documents**," and "**materials**," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

Collectors of Child Pornography

14. Based upon my knowledge, training, and experience in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the collection of child pornography (hereafter "collectors"):
- a. Collectors may receive sexual stimulation and satisfaction from contact with children, or from having fantasies of children engaged in sexual activity or suggestive poses, or from literature describing such activity.
 - b. Collectors may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Collectors typically use these materials for their own sexual arousal and gratification. Collectors often have companion collections of child erotica. Child erotica are materials or items that are sexually suggestive and arousing to pedophiles, but which are not in and of themselves obscene or pornographic. Such items may include photographs of clothed children, drawings, sketches, fantasy writings, diaries, pedophilic literature and sexual aids.

- c. Collectors who also actively seek to engage in sexual activity with children may use these materials to lower the inhibitions of a child they are attempting to seduce, convince the child of the normalcy of such conduct, sexually arouse their selected child partner, or demonstrate how to perform the desired sexual acts.
- d. Collectors almost always possess and maintain their “hard copies” of child pornographic images and reference materials (e.g., mailing and address lists) in a private and secure location. With the growth of the Internet and computers, a large percentage of most collections today are in digital format. Typically these materials are kept at the collector’s residence for easy access and viewing. Collectors usually place high value on their materials because of the difficulty, and legal and social danger, associated with acquiring them. As a result, it is not uncommon for collectors to retain child pornography for long periods of time, even for years. Collectors often discard child pornography images only while “culling” their collections to improve their overall quality.
- e. Collectors also may correspond with and/or meet others to share information and materials. They may save correspondence from other child pornography distributors/collectors, including contact information like email addresses, and may conceal such correspondence as they do their sexually explicit material.
- f. Collectors prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.
- g. Subscribers to websites that are primarily designed to provide child pornography have a strong likelihood of being collectors of child pornography. This high degree of correlation between subscription and collection behavior has been repeatedly confirmed during several recent nationwide law enforcement initiatives.

Use of Computers and the Internet with Child Pornography

- 15. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, and utilized. It has also revolutionized the way in which child pornography collectors interact with each other, as well the methods that individuals will use to interact with and sexually exploit children. Computers serve four functions in connection with child pornography: production; communication; distribution and storage.

- a. **Production:** Pornographers can now produce both still and moving images directly from a common video camera. The camera is attached, using a cable, directly to the computer using a device called a video capture board. This device turns the video output into a form that is usable by computer programs. The output of the video camera can be stored, manipulated, transferred or printed directly from the computer. The captured image can be edited (*i.e.*, lightened, darkened, cropped, digitally enhanced, *etc.*) with a variety of commonly available graphics programs. The producers of child pornography can also use scanners to convert hard-copy photographs into digital images.
- b. **Communication.** Previously, child pornography collectors had to rely on personal contact, U.S. mail, and telephonic communications in order to sell, trade, or market pornography. Today most communications associated with the trafficking of child pornography occur via the obscurity and relative anonymity of the Internet. A device known as a modem allows any computer to connect to the Internet via telephone lines or broadband Internet connections. Once connected to the Internet, individuals search for and/or offer to distribute child pornography in a wide variety of ways. Many individuals congregate in topic-based Internet chat rooms implicitly or explicitly dedicated to child pornography. Online discussions in these chat rooms are usually done via instant message (or "IM"), and individuals may then establish one-on-one chat sessions involving private messages (or "PMs"), visible only to the two parties, to trade child pornography. These child pornography images may be attachments to the PMs, or they may be sent separately via electronic mail between the two parties. Pedophile websites communicate advertisements for the sale of child pornography, and individuals may order child pornography from these websites using email or send order information from their web browser (using HTTP computer language). Some individuals communicate via Internet Relay Chat (IRC) to discuss and trade child pornography images. It is not uncommon for child pornography collectors to engage in mutual validation of their interest in such material through Internet-based communications.
- c. **Distribution.** Computers and the Internet are the preferred method to distribute child pornography. As discussed above, such images may be distributed via electronic mail (either as an attachment or embedded image), or through instant messages as attachments. Child pornography is regularly downloaded from servers or Usenet newsgroups via a method known as FTP (file transfer protocol). Child pornography images are also distributed from websites via client computers web browsers downloading such images via HTTP (Hyper Text Transfer Protocol). Peer-to-peer networks such as LimeWire and Gnutella are an increasingly popular method by which child pornography images are distributed over the Internet.

- d. **Storage.** The computer's capability to store images in digital form makes it an ideal repository for pornography. A single floppy disk can store dozens of images and hundreds of pages of text. The size of computer hard drives used in home computers has grown tremendously within the last several years. Hard drives with the capacity of two hundred (200) gigabytes are not uncommon. These drives can store thousands of images at very high resolution. Remote storage of these images on servers physically removed from a collector's home computer adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the scene of the crime. Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

Skype

- 16. Skype owns and operates a communication service that transmits voice calls, video, and messages over the Internet. In May 2011, Skype was acquired by Microsoft Corporation, a company based in Redmond, Washington.
- 17. Skype users can make and receive local, long distance, and international phone calls; participate in video chats or send and receive video messages; send and receive short message system (SMS) text messages; and send and receive electronic files including documents, pictures, audio, and video.

NCMEC and Cyber Tipline Reports

- 18. The National Center for Missing and Exploited Children (commonly known as "NCMEC") was founded in 1984 to serve as a clearinghouse on issues related to missing and sexually exploited children. It is currently authorized by Congress to perform 19 programs and services to assist law enforcement, families, and professions find missing children, reduce child sexual exploitation, and prevent child victimization.
- 19. As part of its functions, NCMEC administers the Cyber Tipline. The Cyber Tipline receives leads and tips from the public and Electronic Service Providers regarding suspected crimes of sexual exploitation committed against children. Electronic Service Providers are required by law to report apparent child pornography to law enforcement via the Cyber Tipline. Analysts review these tips and refer them to the appropriate federal, state, and local law enforcement authorities.

FACTS SUPPORTING PROBABLE CAUSE

FRAZIER's Supervised Release

20. On or around April 18, 2011, FRAZIER pled guilty to an indictment filed in the United States District Court for the Southern District of Ohio charging him with one count of receipt of child pornography, in violation of 18 U.S.C. § 2252(a)(2) and (b). On or around July 11, 2012, FRAZIER was sentenced to 84 months imprisonment followed by lifetime of supervised release.
21. On or around September 6, 2018, FRAZIER was released from the custody of the Bureau of Prisons and began his term of supervised release. Since his release, FRAZIER has been supervised by Probation Officer (PO) Christopher Owens of the United States Probation Service in the Southern District of Ohio. Among other conditions, the terms of FRAZIER's supervised release included the following:
 - a. FRAZIER was prohibited from possessing or viewing pornography of any kind.
 - b. FRAZIER was required to seek authorization to purchase and/or use any computer devices. FRAZIER was also required to permit the installation of software to monitor computer activities on any computer that he was authorized to use.
22. Based on information from PO Owens, I have learned the following additional information about FRAZIER's supervised release:
 - a. FRAZIER resides with his mother and mother's boyfriend at 501 N. West Avenue in Sidney, Ohio. PO Owens has conducted regular home visits at this residence and has verified that FRAZIER resides there.
 - b. PO Owens previously provided authorization for FRAZIER to utilize an HP Stream laptop (consistent with the **SUBJECT DEVICE**). Monitoring software utilized by the United States Probation Service was installed on this laptop on or around February 18, 2018.
 - c. FRAZIER later requested and received authorization to utilize a Dell laptop. The monitoring software was installed on this laptop on or around September 4, 2019.
 - d. Around September 2019, FRAZIER told PO Owens that he planned to get rid of his HP Stream laptop. The monitoring software was removed from the HP Stream laptop on or around September 20, 2019. FRAZIER told PO Owens that he was going to take the laptop to a computer store to be destroyed or scrapped. PO Owens asked FRAZIER to provide a receipt or other document to verify the

laptop's disposal. FRAZIER emailed PO Owens a picture of an invoice from the Plug & Play Home Computers store (with an address of 401 East Court Street in Sidney, Ohio). This invoice documented the store's receipt a Mini HP Stream laptop in a blue case from "Frazier" to be scrapped. The invoice was dated on or around September 20, 2019.

- e. Other than the Dell laptop, HP Mini laptop, and a flip-style cellular telephone (which does not have the capability to connect to the Internet), PO Owens has not authorized FRAZIER to utilize any other electronic devices.
- f. PO Owens has utilized the monitoring software installed on FRAZIER's laptops to review FRAZIER's computer activities. Although PO Owens is able to review a significant portion of FRAZIER's computer activities through the software, he is not able to review all of the computers' contents.
- g. In or around April 2019, while reviewing FRAZIER's computer activities on the HP Stream laptop, PO Owens found that FRAZIER was utilizing Skype. PO Owens observed communications between FRAZIER and a female who appeared to be a teenager or young adult. PO Owens did not observe any communications that involved the exchange of sexually explicit content with this female. PO Owens suggested that FRAZIER stop communicating on Skype at that time, and FRAZIER agreed. PO Owens did not observe any additional Skype communications on FRAZIER's laptops since that time. Other than this Skype activity, PO Owens did not observe any other activity on FRAZIER's laptops that appeared to be possible violations of the terms of FRAZIER's supervised release.
- h. FRAZIER has sent emails to PO Owens from the email address frazierc652@gmail.com. In or around December 2018, prior to FRAZIER's purchase of the HP Stream laptop, PO Owens conducted a search of the frazierc652@gmail.com email account and did not locate any messages that would constitute violations of the terms of FRAZIER's supervised release. PO Owens has not conducted any searches of this email account since that time.

Cyber Tipline Reports

- 23. On or around July 6, 2019, Microsoft Corporation filed approximately two reports to NCMEC's Cyber Tipline regarding two suspected child pornography or child exploitation files that were located in a Skype media storage account for the user name of live:frazierc652. Microsoft Corporation reported that the two files were located in the Skype account on or around July 5, 2019. Microsoft Corporation's records identified that the IP address of 71.213.6.203 was utilized by the user at the time that the files were scanned into the live:frazierc652 Skype account. Microsoft Corporation provided the approximately two suspected child pornography or child exploitation files to NCMEC.

24. Microsoft Corporation's Cyber Tipline report, along with the two suspected child pornography or child exploitation files, were originally forwarded to the Cuyahoga County Internet Crimes Against Children (ICAC) Task Force for further examination. I later obtained and reviewed these files. Based on my training and experience, I believe that both of the files depict child pornography. The files are described as follows:
 - a. 8a501865-d032-4636-a837-e80267304744.jpg: The file is an image that depicts what appears to be a female child wearing a blue shirt, but she is nude from the waist down. The child is sitting with her legs straddled, exposing her nude vagina to the camera.
 - b. 8db86d7c-e39f-4568-94c3-30cf3c6626f9.mp4: The file is a video that depicts what appears to be the same female child described above, again wearing a blue shirt but nude from the waist down. The child spreads apart her vagina and starts to masturbate her vagina. The video is approximately ten seconds in duration.
25. Century Link was identified as the Internet Service Provider for the IP address of 71.213.6.203. On or around August 12, 2019, an investigator from the Cuyahoga County ICAC served an administrative subpoena to Century Link requesting subscriber information for this IP address on the date and time that it was utilized by the live:frazierc652 Skype account to access the two child pornography files. Records received in response to the subpoena identified that the account was subscribed to FRAZIER at 501 N. West Avenue in Sidney, Ohio. The email address associated with the subscriber's Century Link account was frazierc652@gmail.com.
 - a. It was noted that the prefix of this email address is consistent with the Skype account name reported by Microsoft Corporation to NCMEC's Cyber Tipline.
 - b. It was also noted that this email address was the same account that FRAZIER reported to PO Owens and that he used to send email messages to PO Owens.

Search of FRAZIER's Residence

26. On or around January 8, 2020, officers of the Sidney Police Department and FBI searched FRAZIER's residence at 501 N. West Avenue in Sidney, Ohio, pursuant to a search warrant authorized by the Sidney (Ohio) Municipal Court. Among other items, a Dell laptop and a desktop computer were seized. During the search, officers observed an empty box for an HP Stream laptop (consistent with the **SUBJECT DEVICE**) in FRAZIER's bedroom.
27. During the execution of the search warrant, FRAZIER agreed to be interviewed after being advised of his Miranda rights. In summary, FRAZIER provided the following information during the interview:

- a. FRAZIER had resided with his mother and mother's boyfriend at 501 N. West Avenue in Sidney, Ohio since approximately September 2018.
- b. FRAZIER had an Internet account that was in his name. He was the only individual who utilized this Internet account, and a password was required to access the account. FRAZIER's mother and his mother's boyfriend utilized a separate Internet account.
- c. FRAZIER utilized the email address cfraziere6@gmail.com.
- d. FRAZIER denied utilizing any social media accounts or messenger applications since he was released from prison in 2018.
- e. FRAZIER currently had a Dell laptop, which was located in his bedroom. FRAZIER previously had an HP Stream laptop (consistent with the **SUBJECT DEVICE**), but he took this laptop to a computer store to be scrapped. FRAZIER stated that the desktop computer that was located in the residence was used by his mother and/or mother's boyfriend, and he denied that he ever used this computer.
- f. FRAZIER originally denied viewing child pornography of any kind since his release from prison in 2018. However, later in the interview and after further discussion, FRAZIER admitted that he had viewed one image of child pornography on one occasion around July 2019. FRAZIER claimed that the following circumstances led him to view the image of child pornography:
 - i. In July 2019, FRAZIER was romantically involved with a woman who will be referred to for purposes of this Affidavit as "Adult Female A". FRAZIER tried to explain his past history involving child pornography to Adult Female A.
 - ii. While Adult Female A was at his residence, FRAZIER asked her if she had ever seen child pornography before. Adult Female A reported that she had never seen child pornography but wanted to understand what FRAZIER had previously viewed.
 - iii. FRAZIER told Adult Female A that before he went to prison, he was able to find child pornography by conducting Internet searches on the Google search engine. He provided her with search terms to utilize in an attempt to find child pornography, including "child porn" and "preteen models". Adult Female A tried to find child pornography by using these search terms on her cellular telephone, but she was unsuccessful.
 - iv. FRAZIER first stated that Adult Female A was able to find an image of child pornography on the "dark web". FRAZIER then alternatively stated

that Adult Female A contacted some of her friends, and that someone sent her a message on her cellular telephone containing child pornography. Adult Female A showed the image to FRAZIER on her cellular telephone and asked if this image was consistent with what FRAZIER previously was interested in and viewed. FRAZIER saw that the image depicted child pornography. FRAZIER claimed that he told Adult Female A to put the image away, and she left his house.

- v. When Adult Female A accessed the child pornography file, she used FRAZIER's Internet service. FRAZIER provided her with the password to access his wireless Internet account. Adult Female A needed to use FRAZIER's Internet service because she did not have a data plan on her telephone.
 - vi. FRAZIER was shown the image that Microsoft Corporation reported to NCMEC's Cyber Tipline. FRAZIER claimed that this was the image that Adult Female A had shown to him.
 - vii. FRAZIER did not tell PO Owens about the image of child pornography that Adult Female A purportedly had shown to him, because he knew this conduct violated the terms of his supervised release.
28. Detective Jon Hoffman of the Sidney Police Department later contacted and interviewed Adult Female A. Adult Female A denied that she ever showed FRAZIER any images of child pornography or that they discussed his previous history of child pornography. She voluntarily provided her cellular telephone to Detective Hoffman and consented for it to be searched. No child pornography files were located during a subsequent search of the device.
29. Officers of the Sidney Police Department have begun searching the computer devices seized from FRAZIER's residence pursuant to the search warrant. The searches have not been completed as of this time. However, during a preliminary review of the Dell laptop, user accounts were found saved on the device for the email addresses frazierc652@gmail.com and cfraziere6@gmail.com.

Seizure of the SUBJECT DEVICE

30. As detailed above, FRAZIER sent PO Owens a picture of an invoice that indicated that FRAZIER took his previous HP Stream laptop to the Plug & Play Home Computers store (located at 401 East Court Street in Sidney, Ohio) to be scrapped.
31. On or around January 14, 2020, Detective Hoffman contacted an employee of the Plug & Play Home Computers store and inquired if FRAZIER had brought an HP Stream Laptop

to the store to be scrapped. The employee confirmed that FRAZIER had in fact brought the laptop to the store. The employee identified that the laptop was still at the store and had not yet been destroyed or electronically altered. The employee located the laptop – that being the **SUBJECT DEVICE** – and voluntarily turned it over to Detective Hoffman.

32. After collecting the **SUBJECT DEVICE**, Detective Hoffman secured it at the Sidney Police Department. On or around January 17, 2020, I collected the **SUBJECT DEVICE** from the Sidney Police Department and secured it at the FBI's office located at 7747 Clyo Road in Centerville, Ohio. The **SUBJECT DEVICE**'s electronic contents have not been accessed or searched while in the law enforcement's custody.

Conclusion Regarding Use of Accounts and Devices

33. Based on all of the information detailed above, there is probable cause to believe that FRAZIER is the user of the live:frazierc652 Skype account. There is also probable cause to believe that FRAZIER utilized this Skype account to intentionally possess and receive child pornography.
34. Again based on all of the information detailed above, there is probable cause to believe that FRAZIER is the user of the **SUBJECT DEVICE**. As detailed above, the **SUBJECT DEVICE** was the only device with Internet access that FRAZIER purportedly utilized at the time that child pornography files were discovered by Microsoft in the live:frazierc652 Skype account (as detailed above). Based on this and other information detailed in the Affidavit, there is probable cause to believe that the **SUBJECT DEVICE** may contain evidence of FRAZIER's child pornography activities.

Additional Background Information on Searches of Computers

35. Based on my training and experience, I know that collectors of child pornography often maintain their collections for long periods of time. In addition, computer evidence typically persists for long periods of time, and computer data can often be recovered from deleted space (as further detailed above).
36. Based on my training and experience, individuals involved in child exploitation schemes often utilize social media accounts, email addresses, messenger applications, and dating websites as a means to locate and recruit victims. They then use the chat functions on these websites, as well as email accounts and other messenger applications, to communicate with their victims. Such communications provide a means of anonymity to protect the subjects' identities and to conceal the communications from the victims' parents.
37. Also based on my training and experience, I know that individuals involved in child exploitation offenses utilize a variety of threats and manipulation techniques to compel

their victims to engage or continue engaging in the illicit sexual activities (including the production of child pornography). These threats and manipulations are intended to control the victims and their activities, prevent them from stopping the activities, and prevent them from contacting law enforcement officers. It is common for such offenders to threaten that if the victims end the illicit sexual activities, the offenders will harm the victims and their family members and / or bring notoriety and shame to the victims by exposing the victims' involvement in the sexually explicit conduct.

38. In my experience, individuals involved in child exploitation schemes often communicate with others involved in similar offenses via e-mail, social media, and other online chatrooms. I have seen examples of cases where such individuals have communicated with other child predators about their sexual fantasies and prior sexual activities with juveniles. I have also seen cases where such individuals have communicated with others about their remorse and regret for their activities. Both types of communications provide material evidence in child exploitation cases in that they provide admissions of guilt.
39. In my experience, individuals often attempt to obtain child pornography from a variety of sources, including from those with whom they communicate via email, social media sites, Internet chat programs, and on Internet bulletin boards; Internet P2P file sharing programs; Internet websites; and other sources. Evidence of multiple aliases, accounts, and sources of child pornography can often be found in the subjects' email communications. Evidence of the multiple aliases, accounts, and sources of child pornography are often found on the computer devices located at the offenders' residences, in their vehicles, and on their persons.
40. In my experience, I know that many laptops store information related to IP addresses and Wi-Fi accounts that the telephone accessed and GPS data. This information helps in identifying the subjects' whereabouts during the criminal activities and the travels they took to get to these locations.
41. Based on my training and experience, I know that providers of cellular telephone service and Internet Service Providers often send their customers monthly billing statements and other records. These statements and records are sometimes mailed to the customers' billing addresses and other times are emailed to the customers' email accounts. Individuals often maintain these documents in their residences and/or on their computers. These documents can be materially relevant to investigations of child exploitation offenses in that they provide evidence of the Internet and cellular telephone accounts utilized in furtherance of the crimes.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

42. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via

the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

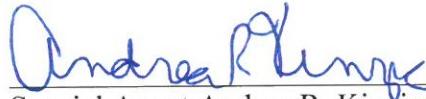
43. There is probable cause to believe that things that were once stored on the **SUBJECT DEVICE** may still be stored there, for at least the following reasons:
- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
 - b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
 - c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
 - d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”
44. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the **SUBJECT DEVICE** was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the **SUBJECT DEVICE** because:
- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
 - c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
 - d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
 - e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.
45. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.
46. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement’s possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

47. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence of a crime; contraband, fruits of crime, or other items illegally possessed; property designed for use, intended for use, or used in committing a crime or violations of federal law; may be located on the **SUBJECT DEVICE**, as described in Attachment A, in violations of 18 U.S.C. §§ 2252(a)(4)(B) and (b)(1), 2252A(a)(5)(B) and (b)(1), 2252(a)(2)(B) and (b)(1), and 2252A(a)(2) and (b)(1)
48. I, therefore, respectfully request that the attached warrant be issued authorizing the search and seizure of the items listed in Attachment B.



Special Agent Andrea R. Kinzig
Federal Bureau of Investigation

SUBSCRIBED and SWORN
before me this 30 of January 2020



SHARON L. OVINGTON
UNITED STATES MAGISTRATE JUDGE